

(19) 日本国特許庁 (JP)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表2010-506245

(P2010-506245A)

(43) 公表日 平成22年2月25日 (2010.2.25)

(51) Int.Cl.	F I	テーマコード (参考)
G06K 19/10 (2006.01)	G06K 19/00 R	2C005
B42D 15/10 (2006.01)	B42D 15/10 521	5B035
G06K 19/07 (2006.01)	B42D 15/10 501A	
G06K 19/08 (2006.01)	G06K 19/00 J	
	G06K 19/00 S	
審査請求 未請求 予備審査請求 未請求 (全 14 頁) 最終頁に続く		

(21) 出願番号 特願2009-513844 (P2009-513844)
 (86) (22) 出願日 平成19年6月3日 (2007.6.3)
 (85) 翻訳文提出日 平成21年1月8日 (2009.1.8)
 (86) 国際出願番号 PCT/IL2007/000676
 (87) 国際公開番号 W02007/141779
 (87) 国際公開日 平成19年12月13日 (2007.12.13)
 (31) 優先権主張番号 60/804, 174
 (32) 優先日 平成18年6月8日 (2006.6.8)
 (33) 優先権主張国 米国 (US)

(71) 出願人 508359561
 ペレド アムラム
 イスラエル, 52226 ラマト ガン,
 アルフ ダビット2
 (74) 代理人 100081053
 弁理士 三俣 弘文
 (72) 発明者 ペレド アムラム
 イスラエル, 52226 ラマト ガン,
 アルフ ダビット2
 Fターム (参考) 2C005 HB01 HB02 HB20 JA02 MB01
 MB03 MB04 MB10 SA06 SA14
 SA15
 5B035 AA13 AA14 BB09 BC00 BC01
 CA04 CA05 CA06 CA11

最終頁に続く

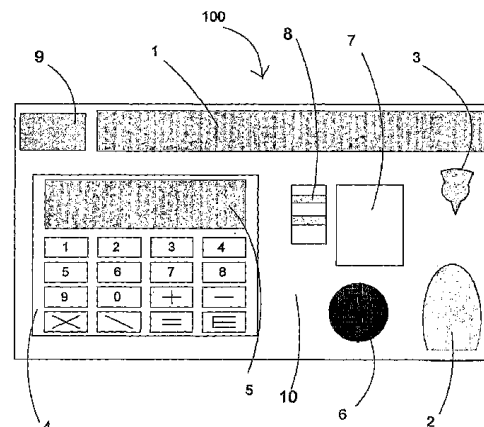
(54) 【発明の名称】 コンピュータベースのクレジット・カード

(57) 【要約】

【課題】 IDカード特にクレジット・カードの不正な使用を阻止すること。

【解決手段】 本発明のコンピュータベースのカードは、(a) 平坦で薄い四角形のカード本体と、(b) 前記カード本体に組み込まれた指紋スキャナ/識別装置と、前記指紋スキャナ/識別装置は、前記コンピュータベースのカードの正規の所有者の指紋に関連するデータでプログラムされており、(c) 前記カード本体に組み込まれたマイクロ・コンピュータと、前記マイクロ・コンピュータは、前記コンピュータベースのカードの正規の所有者の所定の個人コードからなる個人識別番号と、一定の順序で配列されたランダムな1回使用のコード群で予めプログラムされており、(d) 前記カード本体に組み込まれた電源とを有する。

【選択図】 図2



【特許請求の範囲】**【請求項 1】**

コンピュータベースのカードにおいて、

(a) 平坦で薄い四角形のカード本体と、

(b) 前記カード本体に組み込まれた指紋スキャナ / 識別装置と、

前記指紋スキャナ / 識別装置は、前記コンピュータベースのカードの正規の所有者の指紋に関連するデータでプログラムされており、

(c) 前記カード本体に組み込まれたマイクロ・コンピュータと、

前記マイクロ・コンピュータは、前記コンピュータベースのカードの正規の所有者の所定の個人コードからなる個人識別番号と、一定の順序で配列されたランダムな 1 回使用のコード群で予めプログラムされており、

(d) 前記カード本体に組み込まれた電源と、

を有する

ことを特徴とするコンピュータベースのカード。

【請求項 2】

(e) 前記カード本体に組み込まれた磁気ストリップ

をさらに有し、

前記磁気ストリップは、コンピュータベースのカードの正規の所有者に関連するデータで予めプログラムされている

ことを特徴とする請求項 1 記載のコンピュータベースのカード。

【請求項 3】

(f) 前記マイクロ・コンピュータに記憶されているデータを表示する第 1 表示スクリーン

をさらに有する

ことを特徴とする請求項 2 記載のコンピュータベースのカード。

【請求項 4】

前記マイクロ・コンピュータは、コンピュータベースのカードの正規の所有者の顔写真を表すデジタルデータで予めプログラムされている

ことを特徴とする請求項 3 記載のコンピュータベースのカード。

【請求項 5】

(g) 前記コンピュータベースのカードの正規のカード所有者の顔写真を表示するよう構成される第 2 表示スクリーン

をさらに有する

ことを特徴とする請求項 4 記載のコンピュータベースのカード。

【請求項 6】

前記マイクロ・コンピュータは、クレジット・カードの番号で予めプログラムされている

ことを特徴とする請求項 5 記載のコンピュータベースのカード。

【請求項 7】

前記クレジット・カードの番号は、16桁である

ことを特徴とする請求項 6 記載のコンピュータベースのカード。

【請求項 8】

プリントされたカード番号もなく、

クレジット・カードの番号表示もない

ことを特徴とする請求項 6 記載のコンピュータベースのカード。

【請求項 9】

前記指紋スキャナ / 識別装置は、活性化スイッチとして機能する

ことを特徴とする請求項 5 記載のコンピュータベースのカード。

【請求項 10】

前記指紋スキャナ / 識別装置は、コンピュータベースのカードの正規の所有者の指

10

20

30

40

50

紋に関連するデータと、前記指紋スキャナ／識別装置によってスキャンされた指紋に関連するデータとを比較して、両方の指紋が、所定の確率で、同一人物に属するか否かを決定する

ことを特徴とする請求項 5 記載のコンピュータベースのカード。

【請求項 1 1】

前記マイクロ・コンピュータは、コンピュータベースのカードの正規の所有者の指紋に関連するデータと、前記指紋スキャナ／識別装置によってスキャンされた指紋に関連するデータとを比較して、両方の指紋が、所定の確率で、同一人物に属するか否かを決定する

ことを特徴とする請求項 5 記載のコンピュータベースのカード。

10

【請求項 1 2】

前記マイクロ・コンピュータは、前記個人識別番号をマイクロ・コンピュータに入力することにより、前記マイクロ・コンピュータは、1 回使用のコードを新たな 1 回使用のコードで置換して、前記新たな 1 回使用のコードを表示し、前記新たな 1 回使用のコードのコピーを前記磁気ストリップに記憶させる

ことを特徴とする請求項 5 記載のコンピュータベースのカード。

【請求項 1 3】

(e) 前記カード本体に組み込まれたデジタル出力ユニットをさらに有し、

前記デジタル出力ユニットは、コンピュータベースのカードの正規の所有者に関連するデータで予めプログラムされている

ことを特徴とする請求項 1 記載のコンピュータベースのカード。

20

【請求項 1 4】

前記マイクロ・コンピュータは、前記個人識別番号をマイクロ・コンピュータに入力することにより、前記マイクロ・コンピュータは、1 回使用のコードを新たな 1 回使用のコードで置換して、前記新たな 1 回使用のコードを表示し、前記新たな 1 回使用のコードのコピーを前記デジタル出力ユニットに記憶させる

ことを特徴とする請求項 1 3 記載のコンピュータベースのカード。

【請求項 1 5】

前記第 2 表示スクリーンは、少なくとも 3 0 ピクセル × 4 0 ピクセルのアレイを有する

ことを特徴とする請求項 5 記載のコンピュータベースのカード。

30

【請求項 1 6】

(h) 前記カード本体上に配置された視覚的なロゴと、

(i) 前記カード本体上に配置された個人識別可視情報と

をさらに有する

ことを特徴とする請求項 1 5 記載のコンピュータベースのカード。

【請求項 1 7】

(a) 以下を含むコンピュータベースのカードを用意するステップと、

(i) 平坦で薄い四角形のカード本体と、

(i i) 前記カード本体に組み込まれた指紋スキャナ／識別装置と、

前記指紋スキャナ／識別装置は、前記コンピュータベースのカードの正規の所有者の指紋に関連するデータでプログラムされており、

前記指紋スキャナ／識別装置は、コンピュータベースのカードの正規の所有者の指紋に関連するデータと、前記指紋スキャナ／識別装置によってスキャンされた指紋に関連するデータとを比較して、両方の指紋が、所定の確率で、同一人物に属するか否かを決定し、

前記指紋スキャナ／識別装置は、活性化スイッチとして機能し、

(i i i) 前記カード本体に組み込まれた磁気ストリップと、

前記磁気ストリップは、コンピュータベースのカードの正規の所有者に関

40

50

連するデータで予めプログラムされており、

(i v) 前記カード本体に組み込まれたマイクロ・コンピュータと、

前記マイクロ・コンピュータは、前記コンピュータベースのカードの正規の所有者の所定の個人コードからなる個人識別番号と、一定の順序で配列されたランダムな 1 回使用のコード群で予めプログラムされており、

前記マイクロ・コンピュータは、前記個人識別番号をマイクロ・コンピュータに入力することにより、前記マイクロ・コンピュータは、1 回使用のコードを新たな 1 回使用のコードで置換して、前記新たな 1 回使用のコードを表示し、前記新たな 1 回使用のコードのコピーを前記磁気ストリップに記憶させ、

(v) 前記カード本体に組み込まれた電源と、

(b) 前記コンピュータベースのカードを、その正規のカード所有者の指を指紋スキャナ / 識別装置に押しつけることにより、活性化するステップと、

(c) 個人コードをマイクロ・コンピュータに、マイクロ・コンピュータのキーを用いて、入力するステップと、

(d) 前記コンピュータベースのカードを、取引に課金しようとする人に、手渡すステップと、

(e) 前記コンピュータベースのカードをカードリーダーで読みとらせ、クレジットカード番号と一回使用の有効コードをクレジットカード会社に送信するステップと、

(f) 送信されたクレジットカード番号と一回使用の有効コードをクレジットカード会社の記録されたデータと比較するステップと、

(g) 比較した結果、両者が一致した場合、取引の課金を認証するステップとを有する

ことを特徴とする取引に際し課金をする方法。

【請求項 18】

前記コンピュータベースのカードは、

(v i) 前記マイクロ・コンピュータ内に記憶されたデータを表示する第 1 表示スクリーン

をさらに有する

ことを特徴とする請求項 17 記載の方法。

【請求項 19】

(h) 前記コンピュータベースのカードを活性化した後、前記第 1 表示スクリーンの上にクレジット・カードの番号と 1 回使用のコードとを表示するステップ

をさらに有する

ことを特徴とする請求項 18 記載の方法。

【請求項 20】

(i) 前記個人コードを前記マイクロ・コンピュータに入力した後、前記 1 回使用のコードを置換し表示するステップ

をさらに有する

ことを特徴とする請求項 19 記載の方法。

【請求項 21】

前記コンピュータベースのカードは、

(v i i) 前記コンピュータベースのカードの正規のカード所有者の顔写真を表示する第 2 表示スクリーン

をさらに有する

ことを特徴とする請求項 17 記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、クレジット・カード、パスポート、IDカード等のセキュリティに関し

10

20

30

40

50

、特にコンピュータベースのクレジット・カードに関する。

【背景技術】

【0002】

クレジット・カードの個人情報の窃盗による不正使用により、クレジット・カード所有者、クレジット・カードを取り扱い課金する会社、クレジット・カード会社が多大な損害を被っている。

【0003】

他人の個人情報（ID）の窃盗を防止することは、最重要課題である。この為、多種多様な手段および方法が長年に渡り開発されてきた。技術進歩による解決方法は、クレジット・カードと小型の技術要素を具備する他のIDカードとの組み合わせ、生体認証（例、指紋の照合等）のセンサ、適宜のソフトウェアを搭載したデジタル計算ハードウェア、さらにはクレジット・カードで従来から使用されている認証手段（例、署名および個人情報を含む磁気ストリップ等）を用いる。バイオセンサを有するバイオ認証カードおよびユーザーの認証方法は、特許文献1に開示されている。

10

【先行技術文献】

【特許文献】

【0004】

【特許文献1】米国特許公開第200601007067号明細書

【0005】

図1は、従来の生体認証カード20の一実施例の斜視図である。生体認証カード20の一態様は、バイオセンサ21と、メモリ（図示せず）と、マイクロ・プロセッサ（図示せず）とを有するIDカードに関連する。バイオセンサ21は、認証されたユーザーから生体特徴痕跡（signature biometric characteristic）を収集する。メモリは、この生体特徴痕跡を記憶する。マイクロ・プロセッサは、バイオセンサ21とメモリに接続されている。マイクロ・プロセッサは、メモリから生体特徴痕跡を取り出し、この生体特徴痕跡とバイオセンサ21から取得した生体特徴サンプルとの比較を行う。生体認証カード20は、表示スクリーン22を有する。この表示スクリーン22は、カウントダウン24を表示する。カウントダウン24は、表示されたパスワード25が有効である残り時間を示す。キーボード23がマイクロ・プロセッサと通信するユーザー・インターフェースを提供する。

20

30

【0006】

従来技術は、クレジット・カードの所有者、クレジット・カードに課金する会社、クレジット・カード会社のセキュリティを、現在の巧妙なレベルの不正使用に対し十分保護するセキュリティ手段あるいはセキュリティ方法を開示していない。

【発明の概要】

【発明が解決しようとする課題】

【0007】

IDの窃盗を困難にし、一般にIDカード特にクレジット・カードに対し、不正な行為を行うのを阻止する必要性がある。

【課題を解決するための手段】

40

【0008】

本発明によれば、本発明のコンピュータベースのカードは、（a）平坦で薄い四角形のカード本体と、（b）前記カード本体に組み込まれた指紋スキャナ/識別装置と、前記指紋スキャナ/識別装置は、前記コンピュータベースのカードの正規の所有者の指紋に関連するデータでプログラムされており、（c）前記カード本体に組み込まれたマイクロ・コンピュータと、前記マイクロ・コンピュータは、前記コンピュータベースのカードの正規の所有者の所定の個人コードからなる個人識別番号と、一定の順序で配列されたランダムな1回使用のコード群で予めプログラムされており、（d）前記カード本体に組み込まれた電源とを有する。

【0009】

50

本発明の一実施例によれば、本発明のコンピュータベースのカードは、(e) 前記カード本体に組み込まれた磁気ストリップをさらにし、前記磁気ストリップは、コンピュータベースのカードの正規の所有者に関連するデータで予めプログラムされている。

【 0 0 1 0 】

本発明の一実施例によれば、本発明のコンピュータベースのカードは、(f) 前記マイクロ・コンピュータに記憶されているデータを表示する第 1 表示スクリーンをさらに有する。

【 0 0 1 1 】

本発明の一実施例によれば、前記マイクロ・コンピュータは、コンピュータベースのカードの正規の所有者の顔写真を表すデジタルデータで予めプログラムされている。

10

【 0 0 1 2 】

本発明の一実施例によれば、本発明のコンピュータベースのカードは、(g) 前記コンピュータベースのカードの正規のカード所有者の顔写真を表示するよう構成される第 2 表示スクリーンをさらに有する。

【 0 0 1 3 】

本発明の一実施例によれば、前記マイクロ・コンピュータは、クレジット・カードの番号で予めプログラムされている。

【 0 0 1 4 】

本発明の一実施例によれば、前記クレジット・カードの番号は、16桁である。

【 0 0 1 5 】

20

本発明の一実施例によれば、本発明のコンピュータベースのカードは、プリントされたカード番号もなく、クレジット・カードの番号表示もない。

【 0 0 1 6 】

本発明の一実施例によれば、前記指紋スキャナ/識別装置は、活性化スイッチとして機能する。

【 0 0 1 7 】

本発明の一実施例によれば、前記指紋スキャナ/識別装置は、コンピュータベースのカードの正規の所有者の指紋に関連するデータと、前記指紋スキャナ/識別装置によってスキャンされた指紋に関連するデータとを比較して、両方の指紋が、所定の確率で、同一人物に属するか否かを決定する。

30

【 0 0 1 8 】

本発明の一実施例によれば、前記マイクロ・コンピュータは、前記個人識別番号をマイクロ・コンピュータに入力することにより、前記マイクロ・コンピュータは、1回使用のコードを新たな1回使用のコードで置換して、前記新たな1回使用のコードを表示し、前記新たな1回使用のコードのコピーを前記磁気ストリップに記憶させる。

【 0 0 1 9 】

本発明の一実施例によれば、本発明のコンピュータベースのカードは、(e) 前記カード本体に組み込まれたデジタル出力ユニットをさらに有し、前記デジタル出力ユニットは、コンピュータベースのカードの正規の所有者に関連するデータで予めプログラムされている。

40

【 0 0 2 0 】

本発明の一実施例によれば、前記マイクロ・コンピュータは、前記個人識別番号をマイクロ・コンピュータに入力することにより、前記マイクロ・コンピュータは、1回使用のコードを新たな1回使用のコードで置換して、前記新たな1回使用のコードを表示し、前記新たな1回使用のコードのコピーを前記デジタル出力ユニットに記憶させる。

【 0 0 2 1 】

本発明の一実施例によれば、前記第 2 表示スクリーンは、少なくとも 30 ピクセル × 40 ピクセルのアレイを有する。

【 0 0 2 2 】

本発明の一実施例によれば、本発明のコンピュータベースのカードは、(h) 前記

50

カード本体上に配置された視覚的なロゴと、(i) 前記カード本体上に配置された個人識別可視情報とをさらに有する。

【 0 0 2 3 】

本発明の一実施例によれば、本発明のコンピュータベースのカードを用いて取引に際し課金をする方法は、(a) 以下を含むコンピュータベースのカードを用意するステップと、(i) 平坦で薄い四角形のカード本体と、(i i) 前記カード本体に組み込まれた指紋スキャナ / 識別装置と、前記指紋スキャナ / 識別装置は、前記コンピュータベースのカードの正規の所有者の指紋に関連するデータでプログラムされており、前記指紋スキャナ / 識別装置は、コンピュータベースのカードの正規の所有者の指紋に関連するデータと、前記指紋スキャナ / 識別装置によってスキャンされた指紋に関連するデータとを比較して、両方の指紋が、所定の確率で、同一人物に属するか否かを決定し、前記指紋スキャナ / 識別装置は、活性化スイッチとして機能し、(i i i) 前記カード本体に組み込まれた磁気ストリップと、前記磁気ストリップは、コンピュータベースのカードの正規の所有者に関連するデータで予めプログラムされており、(i v) 前記カード本体に組み込まれたマイクロ・コンピュータと、前記マイクロ・コンピュータは、前記コンピュータベースのカードの正規の所有者の所定の個人コードからなる個人識別番号と、一定の順序で配列されたランダムな 1 回使用のコード群で予めプログラムされており、前記マイクロ・コンピュータは、前記個人識別番号をマイクロ・コンピュータに入力することにより、前記マイクロ・コンピュータは、1 回使用のコードを新たな 1 回使用のコードで置換して、前記新たな 1 回使用のコードを表示し、前記新たな 1 回使用のコードのコピーを前記磁気ストリップに記憶させ、(v) 前記カード本体に組み込まれた電源と、(b) 前記コンピュータベースのカードを、その正規のカード所有者の指を指紋スキャナ / 識別装置に押しつけることにより、活性化するステップと、(c) 個人コードをマイクロ・コンピュータに、マイクロ・コンピュータのキーを用いて、入力するステップと、(d) 前記コンピュータベースのカードを、取引に課金しようとする人に、手渡すステップと、(e) 前記コンピュータベースのカードをカードリーダーで読みとらせ、クレジットカード番号と一回使用の有効コードをクレジットカード会社へ送信するステップと、(f) 送信されたクレジットカード番号と一回使用の有効コードをクレジットカード会社の記録されたデータと比較するステップと、(g) 比較した結果、両者が一致した場合、取引の課金を認証するステップとを有する。

10

20

30

【 0 0 2 4 】

本発明の一実施例によれば、前記コンピュータベースのカードは、(v i) 前記マイクロ・コンピュータ内に記憶されたデータを表示する第 1 表示スクリーンをさらに有する。

【 0 0 2 5 】

本発明の一実施例によれば、本発明のコンピュータベースのカードを用いて取引に際し課金をする方法は、(h) 前記コンピュータベースのカードを活性化した後、前記第 1 表示スクリーンの上にクレジットカードの番号と 1 回使用のコードとを表示するステップをさらに有する。

【 0 0 2 6 】

本発明の一実施例によれば、本発明のコンピュータベースのカードを用いて取引に際し課金をする方法は、(i) 前記個人コードを前記マイクロ・コンピュータに入力した後、前記 1 回使用のコードを置換し表示するステップをさらに有する。

40

【 0 0 2 7 】

本発明の一実施例によれば、前記コンピュータベースのカードは、(v i i) 前記コンピュータベースのカードの正規のカード所有者の顔写真を表示する第 2 表示スクリーンをさらに有する。

【 図面の簡単な説明 】

【 0 0 2 8 】

【 図 1 】 従来技術に係る生体認証カードの斜視図。

50

【図 2】本発明の一実施例によるコンピュータベースのクレジット・カードの上面図。

【図 3】本発明の一実施例によるコンピュータベースのクレジット・カードの操作を行う方法のフローチャート。

【図 4 a】図 3 のフローチャートの一部を表すフローチャート。

【図 4 b】図 3 のフローチャートの一部を表すフローチャート。

【図 4 c】図 3 のフローチャートの一部を表すフローチャート。

【発明を実施するために形態】

【0029】

本発明は、セキュリティ・カード、特にコンピュータベースの（クレジット・）カードに関する。他人の個人情報（ID）の窃盗を防止することは、重要なことである。この為、多種多様な手段および方法が長年に渡り開発されてきた。しかし、依然としてこのような防止手段を破る多くの事例が存在する。例えば、IDの窃盗、偽造したあるいは盗んだパスポートを用いて入国するような様々な違法行為、盗んだあるいは偽造したクレジット・カードで一時的な取引を行うケースである。

10

【0030】

本発明によれば、様々な手段のセキュリティは、IDの窃盗を極端に困難にしたり、不正行為を阻止するような手段と方法を組み合わせることにより、さらに向上する。このような不正防止手段は磁気ストリップを含む。この磁気ストリップは、認証を実行する為に、正規の所有者のIDの詳細（例、名前、ID番号、誕生日、性別等）を含む。更に制御手段および生体認証のような付加的な認証手段も含む。特に、指紋による認証や1回使用のコード（符号）の生成用マイクロ・コンピュータがあり、これらは、磁気ストリップあるいはデジタル出力ユニットに記憶されている。

20

【0031】

図 2 は、本発明の第 1 実施例のコンピュータベースのクレジット・カード 100 を示す。同図に示す磁気ストリップ 1 は、正規のカード所有者の個人情報を含む。例えば、国籍、居住都市、姓、名、さらなる詳細情報（例、クレジットカード番号、銀行支店番号、口座番号等）と複数の数字列（例、3桁の数字）とを含む。この3桁の数字は、課金毎に変わる1回使用のコードとして機能する。

【0032】

本発明の他の実施例によれば、クレジット・カード 100 は、デジタル出力ユニットを有する。このデジタル出力ユニットに、1回使用のコード情報がデジタルデータとして転送され、これにより指定されたデジタルカード・リーダでデータを読み取ることができる。

30

【0033】

1回使用のコードの詳細は、カードには示されていないが、クレジット・カード会社のデータベースに記録されている。

【0034】

クレジット・カード 100 のマイクロ・コンピュータ 4 は、メモリ（図示せず）を有する。このメモリに、各クレジット・カード 100 に独自の数千のランダムな1回使用コードを特定の順で記憶する。これと同一順に配列されたランダム符号の同じ列が、クレジット・カード会社のコンピュータメモリに記憶され、取引に際し両者を比較し、これにより取引を認証する。

40

【0035】

クレジット・カード 100 は、生体認証センサを有する。この生体認証センサは、第 1 実施例では指紋スキャナである。指紋スキャナ / 識別装置 2 は、クレジット・カード 100 を活性化する方法として機能する。クレジット・カード 100 は、一旦活性化されると、所定の時間（例、2 分間）活性 / 能動状態を維持する。

【0036】

クレジット・カード 100 が活性化されると、正規のカード所有者の顔写真が第 2 表示スクリーン 7 に表示される。

50

【 0 0 3 7 】

第 2 表示スクリーン 7 は、人の顔の写真を識別可能に表示できる程度の解像度を有する。例えば、この解像度は、 $n \times m$ ($n = 30$ 、 $m = 40$) ピクセル以上である。

【 0 0 3 8 】

クレジット・カード 100 は、マイクロ・コンピュータ 4 を有する。このマイクロ・コンピュータ 4 は、第 1 表示スクリーン 5 を有する。クレジット・カード 100 が活性化あるいは再度活性化される（例、指紋スキャナ / 識別装置 2 に指を押し当てる）と、マイクロ・コンピュータ 4 は、クレジット・カード 100 を取引の為に用いない場合には、計算機としても使用できる。クレジット・カード 100 を取引を行うためクレジット・カードとしての使用を可能とするために、ユーザーは、個人識別番号（PIN）を入力しなければならない。この個人識別番号は、クレジット・カード 100 の正規のカード所有者の一定の個人コードである。この PIN を入力すると、第 1 表示スクリーン 5 は、1 回使用のコードを表示する。この 1 回使用のコードは、3 桁、4 桁あるいはそれ以上の桁の（数字の）組み合わせであり、これは取引を行うために、1 回のみ使用でき、入力後直ちに新たな 1 回使用のコードで置換される。前の 1 回使用のコードは、使用した最後のものである。カードで取引を実行する前に、クレジット・カード 100 を最初に活性化するためには、任意の所定の 1 回使用のコード、例えば、「000」が表示される。

【 0 0 3 9 】

クレジット・カード 100 は、電源 6 を有する。この電源 6 は、電池、太陽電池（バッテリーの存否を問わない）、あるいは他の適宜の電源である。クレジット・カード 100 は、個人識別情報（例、正規のカード所有者の身長と目の色等）の固定表示 8 を有する。さらにクレジット・カード 100 は、クレジット・カード会社のロゴ 3 を有する。

【 0 0 4 0 】

クレジット・カード 100 は、従来のクレジット・カード番号をマイクロ・コンピュータ 4 のメモリ内に記憶する。この番号は、磁気ストリップ 1 の上に、必要によっては、デジタル出力ユニット 9 内に記憶される。従来のクレジット・カード番号は、16 桁で、所定の制限時間間隔で第 1 表示スクリーン 5 の上に表示される。かくしてクレジット・カード上にクレジット・カード番号を表示する必要はない。これは、クレジット・カードのセキュリティのレベルを上げるため、クレジット・カードで一般に使われている手法である。

【 0 0 4 1 】

クレジット・カード 100 の構成要素は、電子回路、データ・パスウェイ（図示せず）により相互接続される。

【 0 0 4 2 】

クレジット・カード 100 の全ての構成要素は、一体となった機械構造を有する。それらが直接相互接続されるか一体に形成されるかを問わずない。また構成要素は、カード本体 10 に搭載されるか一体に構成される。

【 0 0 4 3 】

第 1 表示スクリーン 5 は、銀行口座の貸借情報と 1 回使用のコードを、動作サイクルの終了時に生成した後、示す。

【 0 0 4 4 】

本発明の一実施例により、正規のカード所有者によるクレジット・カード 100 の使用方法を示す。

【 0 0 4 5 】

正規のカード所有者は、以下のステップを実行する。

【 0 0 4 6 】

第 1 ステップ：クレジット・カード 100 の正規のカード所有者は、指で指紋スキャナ / 識別装置 2 を押して、クレジット・カード 100 を駆動する。しかし、取引に課金する準備はできていない。

【 0 0 4 7 】

即ち、指紋スキャナ／識別装置 2 は、活性ボタンとして機能し、クレジット・カード 100 をオン・モードに切り替える。このオン・モードは、所定の時間（例、2 分間）継続する。

【0048】

クレジット・カード 100 の活性化は、他人の指でさらには類似物で、指紋スキャナ／識別装置 2 を押してもできるが、正規のカード所有者の指紋が認識されないと、その後の動作は継続しない。

【0049】

クレジット・カード 100 が活性化されると、情報は、第 1 表示スクリーン 5 に、横に次のように表示される。

10

【0050】

第 1 表示行は、銀行により設定されたクレジット・カードの正規のカード所有者のライン（限度額）である。

【0051】

第 2 表示行は、正規のカード所有者が使える残高を示す。

【0052】

例えば、クレジットライン（貸出し／取引限度額）が 2 万ドルで、正規のカード所有者がこれまでに 5 千ドル使用した場合には、第 1 表示行は 2 万ドルを、第 2 表示行は 1 万 5 千ドルを示す。第 3 表示行は、クレジット・カードの番号（通常 16 桁）と 3 桁（クレジット・カード 100 に表示される最後の 1 回使用のコード）を示す。

20

【0053】

この表示は、ベンダー（売り主側）が、クレジット・カードを非活性化する前に、必要な動作の全てを完了できない場合に必要である。この表示により、ベンダーは、指紋スキャナ／識別装置 2 を押して、クレジット・カードを再度活性化し、課金プロセスを継続する。課金が行われなかった場合には、正規のカード所有者は、取引を行うために表示された最後の 1 回使用のコードの使用を阻止するコマンドを入力できる。

【0054】

これらの表示の例は、本発明の一実施例であり、これに限定されない。

【0055】

第 2 ステップ：マイクロ・コンピュータ 4 のキーを用いて、PIN コードを入力する。この PIN（個人識別番号）コードは、クレジット・カード 100 の正規のカード所有者の一定個人コードである。PIN が入力されると、1 回使用コードが置換されて、新たな 3 桁の数字が、前の 1 回使用コードの代わりに、第 3 表示行の終わりに表示される。更にマイクロ・コンピュータ 4 は、その新たな 1 回使用のコードをアナログデータとして磁気ストリップ 1 に送信する、他の実施例では、デジタルデータとして、デジタル出力ユニット 9 に送る。後者の場合、デジタルカード・リーダの使用が必要である。

30

【0056】

磁気ストリップ 1 は、一定のデータ（例、正規のカード所有者の市、国、名前、ID 番号、クレジット・カード 100 で引き落とされる銀行の口座番号）を含む。

【0057】

クレジット・カードの番号と 1 回使用のコードの番号の可視表示は、取引を行う場合に必要である。例えば、電話による取引、インターネットによる取引、カードから直接データが読み出せずにカード・リーダにより読み出す他の取引に必要である。

40

【0058】

第 3 ステップ：クレジット・カード 100 をベンダーあるいは課金者に手渡す。

【0059】

第 4 ステップ：クレジット・カード 100 をカード・リーダで読み取らせる。通常 19 桁の番号（クレジット・カードの番号（16 桁）と 1 回使用の有効コード（3 桁））が、クレジット・カード会社に転送される。転送されたデータとクレジット・カード会社の記録等の一致が、取引の認証に必要である。多くの組み合わせ（例、2 千桁の数字組み

50

合わせ)が、1回使用のコードとして機能するが、ランダムに生成され、クレジット・カード会社のコンピュータ・メモリとマイクロプロセッサ4のメモリに、両方の記録装置上に同一の順番で記憶されている。

【0060】

前述したように、クレジット・カード100は、次の3種類の数字を用いる。

(a) クレジット・カードの番号、通常16桁のコード。

(b) 個人識別番号(PIN)、通常3桁または4桁のコード。

これら両方のコードとも、マイクロ・コンピュータ4のメモリ内に記憶され、その後、クレジット・カード100が正規のカード所有者に発行される。特別な場合を除いて、クレジット・カード100を使用されている限り、変更されることはない。

10

(c) 1回使用のコード、ランダムに生成された3桁のコード。

【0061】

クレジット・カード100は、ユーザーの銀行口座を管理せず、またその銀行の支店との通信も必要としない。

【0062】

そのコンピュータベースのクレジット・カードが提供する高レベルのセキュリティを崩さないために、コンピュータベースのクレジット・カードは、通信モデムを含まない。

【0063】

クレジット・カード100を実際に使用することなく、課金されるさらなる取引の場合には、クレジット・カード100の残高を手動で更新できる。

20

【0064】

例えば、クレジット・カード会社がチャージした場合(例、金利の変更)である。クレジットラインは、手動では変更できない(クレジット・カード会社または銀行のみが変更できる)。

【0065】

図3は、本発明の一実施例のクレジット・カード100の操作を表すフローチャートである。

【0066】

図のフローチャートの枠は、以下の通りである。

30

四角形の枠は、プロセスまたは状態を表す。

菱形は、判断/決定を表す。

【0067】

図3の点線の3つの領域a、b、cは、それぞれ本発明の操作の特定の部分のみを示す。

【0068】

図4a—4cは、図3のフローチャートの一部を分けて示す。図3は、各四角形と菱形に番号を付しただけで、その中に示された番号は、符号の説明に記載したとおりである。

【0069】

40

以上の説明は、本発明の一実施例に関するもので、この技術分野の当業者であれば、本発明の種々の変形例を考え得るが、それらはいずれも本発明の技術的範囲に包含される。特に、本発明の実施例の説明では、「コンピュータベースのクレジットカード」を例に説明しているが、特許請求の範囲では、単に「コンピュータベースのカード」としている。これは、特許請求の範囲では、IDカード、パスポート等の「クレジットカード」以外のカードも含むことを意図する。特許請求の範囲の構成要素の後に記載した括弧内の番号は、図面の部品番号に対応し、発明の容易なる理解の為に付したものであり、発明を限定的に解釈するために用いてはならない。また、同一番号でも明細書と特許請求の範囲の部品名は必ずしも同一ではない。これは上記した理由による。

【符号の説明】

50

【 0 0 7 0 】

1	磁気ストリップ	
2	指紋スキャナ / 識別装置	
3	ロゴ	
4	マイクロ・コンピュータ	
5	第 1 表示スクリーン	
6	電源	
7	第 2 表示スクリーン	
8	個人識別情報	
9	デジタル出力ユニット	10
2 0	生体認証カード	
2 1	バイオセンサ	
2 2	表示スクリーン	
2 3	キーボード	
2 4	表示されたカウントダウン	
2 5	表示されたパスワード	
1 0 0	コンピュータベースのクレジット・カード	
1 0 1	コンピュータベースのカードは、スタンバイ・モードにあり、「指紋識別」機能が活性化されている。	
1 0 2	識別する為に指を置く。	20
1 0 3	指紋が同定されたかを決定する。	
1 0 4	スタンバイ・モードに戻る。	
1 0 5	コンピュータベースのカードが活性化され、正規のカード所有者の写真がそのコンピュータベースのカード上に表示され、マイクロ・コンピュータが活性化される。	
1 0 6	タイマーが活性化され、所定の時間後、コンピュータベースのカードがスタンバイ・モードに戻る。	
1 0 7	データを認証する為に、磁気ストリップがスキャナーでスキャンされる。	
1 0 8	磁気ストリップのデータと一致があるかを決定する。	
1 0 9	所定の個人識別番号 (P I N) を入力する。	
1 1 0	所定の P I N との一致があるか決定する。	30
1 1 1	1 回使用のコードを入力する。	
1 1 2	1 回使用のコードとの一致があるかを決定する。	
1 1 3	取引を実行する。	
1 1 4	新たな 1 回使用コードを生成し、それをマイクロ・コンピュータのディスプレイである第 1 表示スクリーンに表示する。	

【図 1】

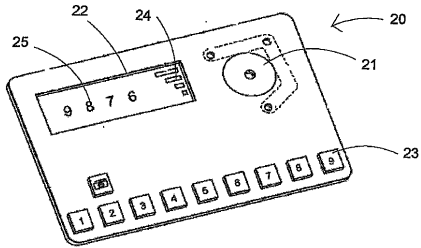


FIG. 1 PRIOR ART

【図 2】

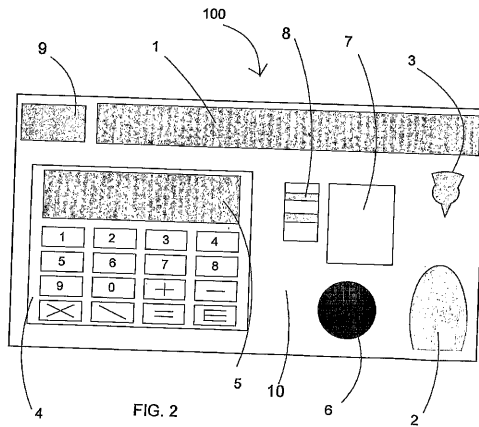


FIG. 2

【図 3】

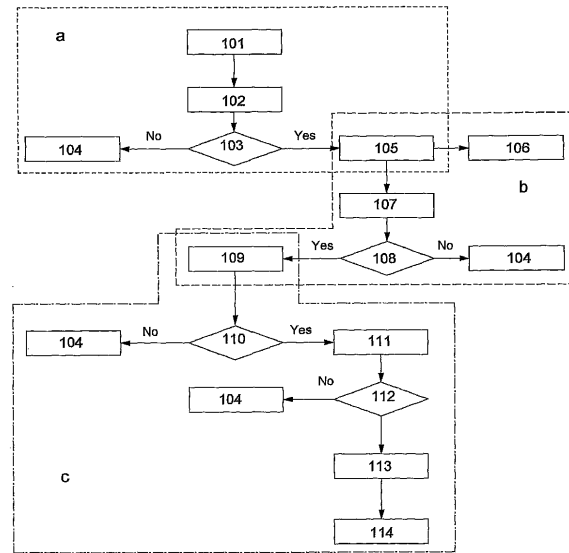
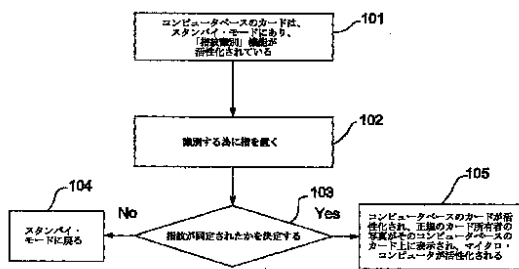
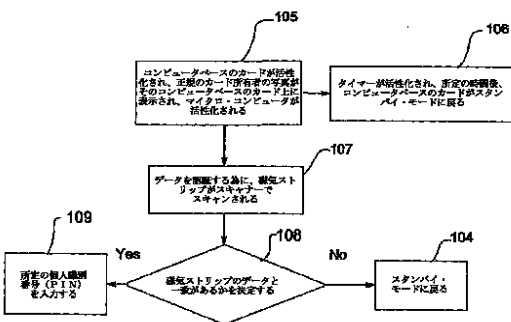


FIG. 3

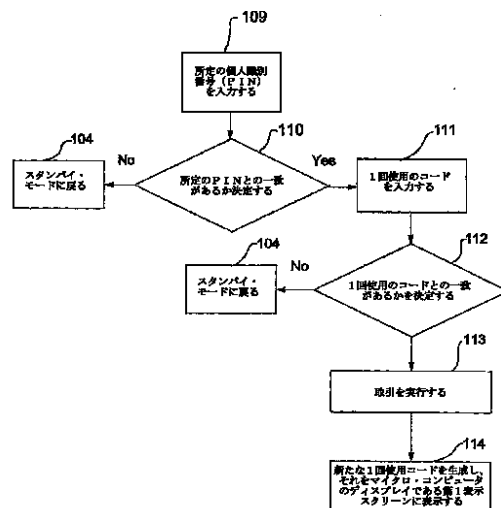
【図 4 a】



【図 4 b】



【図 4 c】



フロントページの続き

(51)Int.Cl.

F I

テーマコード (参考)

G 0 6 K 19/00

F

(81)指定国

AP(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
EP(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OA(
BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH,
CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, K
P, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC
, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW